Instructions for Existing Providers to the Virtual Gateway Services

This document of "things to do" and instructions will help prepare your organization to use the Enterprise Invoice/Service Management (EIM/ESM) business service within the Virtual Gateway.

Please find below a summary checklist of requirements that we ask you to complete in this document. Since you are an existing provider to the Virtual Gateway Services, this checklist does not include some legal forms you have already submitted.

- [ ] **1.** Read and Sign the Enterprise Invoice/Service Management Rider (FORM C).
- [ ] **2.** Read and Complete the Organization Management Form (FORM D).
- [ ] **3.** Read and Complete the User Request Form
- [ ] **4.** Return completed Welcome Package Forms and Agreements to EOHHS Virtual Gateway Operations.

The rest of this document explains in detail the documents we ask you to complete. Before "going live" on EIM/ESM, each organization will need to:

1. READ AND SIGN THE ENTERPRISE INVOICE MANAGEMENT/ENTERPRISE SERVICE MANAGEMENT RIDER (FORM C).

Certain business services require organizations to agree to additional terms and conditions of use, which are included in riders to the standard Virtual Gateway Services Agreement. The Virtual Gateway Services Agreement sets forth the terms and conditions to which your organization must agree in order to access the Virtual Gateway. Since you are an existing provider to the Virtual Gateway Services, you have already submitted this form. The EIM/ESM rider must also be signed by your organization, and will become incorporated into the Virtual Gateway Services Agreement.

2. COMPLETE THE SECURITY FORMS

The EIM/ESM Provider Deployment Team will hold workshops and conference calls to assist providers in completing the Security Forms. An initial schedule of workshops and calls is provided in the Welcome Package. If you need information on the schedule for these workshops and calls, please call Virtual Gateway Customer Service at 1-800-421-0938. We understand that this is a lot of information. Please call us for help if you need it!

2.1 Security Overview

Enterprise Invoice/Service Management (EIM/ESM) is a web-based service, which means it can be accessed from anywhere. As a result, special steps have to be taken to ensure that the data stored within it is secure and accessible only to those who are authorized to have such access. Unlike paper copies of invoices, contracts, client rosters etc. that can be locked in a filing cabinet, the online copies have to be secured electronically – this is done via a combination of *Organization Management, Security Roles*, and *Data Access* rules.

An **Organization** is a legal entity or location that users are associated with. It can be a parent corporation, a site office where services are rendered (e.g. group home) or where billing occurs (e.g. regional billing office).

This is the information documented on the Organization Management Form (Form D). Organizations in EIM/ESM can be divided into sub-organizations, with staff members employed at the appropriate levels. A sub-organization is a site that has a direct relationship to a parent organization – i.e., it is *owned and operated* by the parent organization. For example, a provider organization can have multiple facilities or sites where services are delivered. **An organization should be documented on the form if it meets at least one of the following criteria:**

- EIM/ESM will be accessed there
- Clients are enrolled there
- Clients receive services there (excluding personal homes of clients)

A **User** is an individual associated with one or more organizations who will have access to the system in order to complete their job duties.

Security Roles define the user's business functions in the system and control what the user can and cannot *do* in EIM/ESM. *This is the information documented on the User Request Form (URF).* For example, the "Invoice Reviewer" security role enables the individual to review invoices in the system, but they cannot create or edit them. The user must be assigned the "Invoice Manager" role to be able to create and edit invoices. A user can have more than one security role and a security role can be associated with more than one user. A user should be assigned only the roles relevant to his or her job function.

Data Access rules control what the user can and cannot *see* in EIM/ESM. The data access rules that are predefined in the system consider the user's organizational relationship to control what data records a user has access to see. For example, data access rules ensure that an "Invoice Reviewer" can review invoices for his/her organization and any organizations under it, but cannot view invoices for other provider organizations. This is the way the Organization Management Form (Form D) and the URF are connected.

The combination of organization management structures, security roles, and data access rules secure the EIM/ESM service so users perform only the system functions that they are authorized to perform, and see only the specific data records that they are authorized to see. To that end, it is necessary that the organization structure and security roles are thoughtfully coordinated to permit appropriate access to system functionality and data. We recommend that you review the URF instructions (2.3) before completing the Organization Management Form. This will give you a better understanding of how the two forms relate to each other.

2.2 Organization Management Form (FORM D)

This form identifies the main (parent) provider organization and whether that organization has multiple sites under it (sub-organizations). The hierarchical relationship between these sites is relevant to how security roles are eventually assigned within the EIM/ESM service.

2.2.1 Completing the Organization Management Form

You will need to complete one organization management form for your organization. This form should be completed comprehensively, i.e., it should reflect the entire provider organization as it pertains to all Purchase of Service EOHHS contracts. The majority of the organization management effort occurs in preparing a provider to go live with the EIM/ESM service for the first time. If and when a provider goes live again with additional contracts, the organization management structure can be revisited for validation. Nonetheless, it is important that the provider organization structure be captured accurately, and in its entirety, the first time it is completed, because it will serve as the foundation for security access.

The first step to compiling accurate and complete information is to identify people who can validate the organization management structure for your organization and its affiliates. These people will then need to:

- Document the structure of your organization, identifying your "parent" organization and then all of its sub-organizations (as many tiers as needed). As mentioned earlier, a sub-organization is a site that has a direct relationship to a parent organization – i.e., it is *owned and operated* by the parent organization. Furthermore, a sub-organization should be documented if EIM/ESM will be accessed there, clients are enrolled there, or services are delivered there (excludes personal homes of clients). In addition, you may create sub-organizations at one physical location to separate security access. (See Figure 1, Tier 2 for an example)

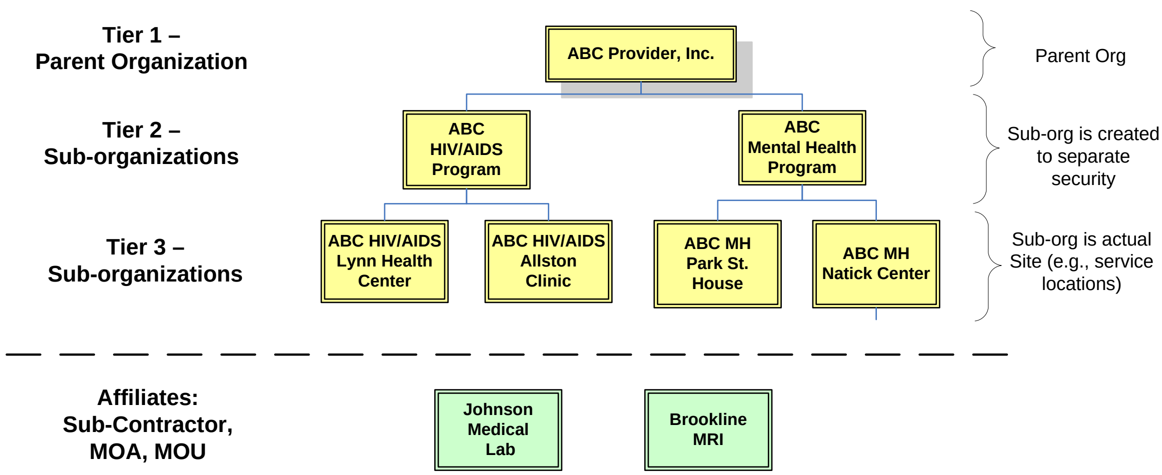
- List all affiliates. Affiliates will include organizations that may deliver services, enroll clients, or perform billing on your behalf, but are *NOT owned and operated* by your parent organization. Note that information on affiliates is *only necessary if:*
  - ✓ you wish to have staff at affiliate organizations access EIM/ESM directly
  - ✓ clients are directly enrolled in those organizations
  - ✓ clients receive services at those affiliate locations

The rest of this section explains in detail the information needed to complete the Organization Management Form.

Tips

Prior to completing the form, we recommended that you develop or verify your Organization Chart that represents your organization's structure. A sample chart is included in Figure 1 (This is also represented on the Example tab on the form.):

Figure 1



Field-by-field Instructions

The <u>first line</u> of the sheet is for your parent organization's information. The rest are for the sub-organizations and affiliates, if any.

Name* – For the overall parent organization, this is the official name of your organization (e.g., ABC Provider, Inc). Names of sub-organizations should start with the short name of the immediate parent org (e.g., ABC Mental Health if it is the Mental Health Program, ABC HIV/AIDS, if it is the HIV/AIDS program).

Short Name* – The abbreviated, or "doing business as" name for your organization (e.g., ABC if it is ABC Provider Inc, ABC HIV/AIDS if it is ABC HIV/AIDS program).

Parent Organization or Affiliate – Complete this field for sub organizations and affiliates as follows:

- **Sub-organizations:** If an organization is a sub-organization, please include the *immediate* parent organization's short name in this column. An immediate parent is the organization that is one level above the sub-organization being described (e.g., ABC HIV/AIDS is the immediate parent of ABC HIV/AIDS Lynn Health Center).
- **Affiliates:** If you identified an organization as an affiliate with whom you subcontract, please mark the column with 'Affiliate'. Once again, information on affiliates is only necessary if you wish to have staff at your affiliate organizations access EIM/ESM directly, clients are directly enrolled in those organizations, or clients receive services at those affiliate locations.

Affiliate Type – If you specified that a sub-organization is an "Affiliate", select what your contract relationship is with that provider: Sub-contractor, Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU).

VCC # – Provide your vendor code (VCC#). You only need to complete the VCC on the parent line of the template (e.g., ABC Provider, Inc.).

Address Line 1* – Street address or P.O. Box

Address Line 2* – Additional information such as suite number or floor number

City – self-explanatory

State – self-explanatory

Zip Code – five digit code

*Note:

- Legal Name and Short Name have a 35 Character Limit
- Address Line 1& 2 have a *combined* 30 Character Limit
- Punctuation and symbols (e.g. # . ,) are not permitted throughout the form

2.2.2 Return the Completed Form to the Virtual Gateway Operations Team

- Save the completed form by adding your parent organization's **short name** and the **date** (MMDDYY) to the end of the filename (e.g., *EIM Org Mgt Structure Example and Form – ABC 052507.xls*)
- Return the form to Virtual Gateway Operations via email at virtualgatewaydeployment@state.ma.us

2.3 User Request Forms (URFs)

Once the Organization Management Form is complete, the URFs are used to identify specific individuals who will be using the EIM/ESM service at *each* of the organizations and sub-organizations identified in the Organization Management Form and assign them security roles that correspond to their job function. The URFs are used to add, change, or delete individual user account information for EIM/ESM access through the Virtual Gateway. The Virtual Gateway will use this information to create an appropriate login (username and password) for the personnel who will be using the EIM/ESM service.

Additionally, URFs will identify who needs training and their training course requirements. Training is mandatory for all EIM/ESM users prior to Go-Live. Training details will be provided in a later communication. The earlier the URFs are submitted, the earlier users will be able to register for training.

2.3.1 Completing the User Request Forms

You will need to complete **one URF for each organization and sub-organization** where users are assigned. The steps for completing the URFs and assigning security roles are as follows:

- **Step One:** Complete the Organization Management form.
- **Step Two:** Refer to the ***"FY09 Contract Go-Live Schedule (click here)"*** to identify which contracts are going live in FY09. This list indicates the agency a contract is associated with. For the relevant contracts, you will identify specific individuals who will be using the EIM/ESM service at *each* of the organizations and sub-organizations identified on your Organization Management Form. Please note the following points when completing URFs:
  - A separate URF must be completed for each organization, "org" (organization or sub-organization), where users are assigned. This means that if you have users at the parent level and the sub-organization level, then you will need to submit a separate URF for each org.
  - Only staff that will be directly accessing EIM/ESM needs to be assigned.
  - If a staff person works at multiple sites, they will have to be included on the URF for each of those sites, or be included on the URF of a parent site.
  - It is very important that the organization's name is recorded, as it is listed under the "Name" column under the Organization Management Form (Form D), on each URF (there is a space for this on the bottom of the URF). The org name can refer to the parent organization or to any of the sub-organizations under it.
- **Step Three**: On the URF complete the following information for each user:
  1. Full name (first name, last name and if applicable middle initial)
  2. Month and day of birth for the PIN
  3. Last 4 digits of SSN (used **only** to prevent user duplication)
  4. Work e-mail address
  5. Work phone number
- **Step Four**: For each user listed you will need to assign specific roles according to their business functions. Please follow the guidelines below when assigning roles.
  - A user must have at least one role assigned to them, but in most cases it will be more than one. ***Note: Please refer to the Appendix for a complete list of the roles, their definitions, and specific required roles. The URF also has a Roles tab with role definitions.***
  - Remember, users should only be able to access functionality applicable to their job function. However, you must also ensure that users can perform their job function without limitation.
  - Accessing Reports: Every user that needs access to reports must be assigned the security roles that will enable them to view the relevant reports. These security roles are listed separately on the URF (e.g. Cost Reimbursement Reports, SDR Reports, etc.).

  For each **role** assigned, type

  - **A** to designate an additional role assignment. *If this is your first time completing the URF, please enter **A** for all users.*

  - **E** to indicate that the role has already been assigned through the Virtual Gateway.
  - **D** to remove an existing role assignment

- **Step Five**: For each **user**, check **one** box in the columns labeled 'New', 'Modify', or 'Deactivate' according to the following definitions:
  - **New User–** Designates first time user role assignments and initiates the creation of a new security account at this particular organization. *If this is your first time completing the URF, please check the 'New' box for all users.*
  - **Modify Existing User –** Modifies an existing user's security roles by assigning additional roles or removing existing roles. The 'Modify' box can be used in the future to indicate changes to a user's roles.
  - **Deactivate Existing User –** Deactivates an existing user's security account and all of its associated roles. The 'Deactivate' box can be used to indicate that a staff member is no longer employed by an organization or if the employee's job changes and the person no longer uses EIM/ESM. A deactivated user will no longer be able to access the system.

2.3.2 Return the Completed URF to the Virtual Gateway Deployment Team

- Save the completed URF by adding the applicable parent or sub organization's **short name** and the **date** (MMDDYY) to the end of the filename (e.g., *user_request_form– ABC 052507.xls*)
- Return the form to Virtual Gateway Operations via email at virtualgatewaydeployment@state.ma.us
- No wet signature is needed to submit the form to Virtual Gateway Operations. However, you must keep a copy of each URF, signed by the Access Administrator, within your organization's records.

3. RETURN COMPLETED WELCOME PACKAGE FORMS AND AGREEMENTS TO EOHHS VIRTUAL GATEWAY OPERATIONS.

Please mail the original executed *EIM/ESM Rider* ***(FORM C)*** to the following address:

EOHHS Virtual Gateway Operations
2 Boylston Street, 6th Floor
Boston, Massachusetts 02116

Please email the *Organization Management Form* ***(FORM D),*** and *URF Forms* to:

virtualgatewaydeployment@state.ma.us

For additional information on the EIM/ESM service go to http://mass.gov/eohhs and click on the **For Providers** tab at the top of your screen, then click **EIM/ESM: Get Started** on the right side of your screen. Among other links you will the find Newsletters, the EIM/ESM Fact Sheet, Frequently Asked Questions (FAQs), and the Virtual Gateway System Requirements available for download.

A dedicated Provider Access Lead (PAL) will contact you soon to offer support. In the meantime, if you have any questions or need additional assistance, please do not hesitate to contact Virtual Gateway Customer Support at (800) 421-0938.

Appendix: URF Roles & Role Descriptions

This Appendix describes the roles that are available to system users. User roles control what someone is authorized to "do" in the system. The URF includes a comprehensive list of roles currently available in EIM/ESM; however, in many cases, only a subset of these roles will be relevant to your provider organization. Please only select roles which are relevant for your provider organization. You can reference the ***"FY09 Contract Go-Live Schedule (click here)"*** to find which contracts are going live in FY09 for your Provider Organization. The major categories of roles are as follows:

- Common Roles – these roles are applicable to all contract types
- EIM Roles
  - Cost Reimbursement – these roles are applicable to providers going-live with Cost Reimbursement contracts
  - Unit Rate - these roles are applicable to providers going-live with Unit Rate contracts
    - Note: a few of the Unit Rate roles apply to DPH providers only
- ESM Roles –these roles are applicable to providers going-live with ESM functionality for management of client data

Key Terms

- Review: Users have read-only access to data
- Manage: Users can create/edit/delete the data
- Release: Users can submit for authorization
- Authorize: Users can review and give final signatory approval to submit to agency

Required Roles (*)

At least one person at the organization needs to have the roles listed below: (You can have more that one and that is highly encouraged for back up purposes)

Required Common Roles

- Contract Reviewer
- Provider PRC Reviewer
- Staff Manager
- EIM Reports

Required Cost Reimbursement Roles

- Invoice Authorizer
- Invoice Manager

Required Unit Rate Roles

- SDR Authorizer
- SDR Location Manager / SDR Manager
- SDR Release

Common Roles	
Contract Reviewer *	• Users with this role may review all contract details, including line item budgets, maximum obligations, sub contractors, affiliates, fund allocations, Ready Pay rates (if applicable) and amendments. • *This role is required for provider staff members authorized to request line item amendments.* • **At least one user at all provider organizations must possess this role.**
Provider PRC Reviewer *	• Users with this role may review a Payment Request for Commodity (PRC), into which EIM/ESM "bundles" invoices prior to making them available for agency review. • *Invoice authorizers, invoice managers, and others who track payment status should be given this role.* • **At least one user at all provider organizations must possess this role.**
Staff Manager *	• Users with this role may add staff names to drop down lists within the Personnel Summary Report. • *The role involves considerable data entry and should be given to persons familiar with staffing details.* • **At least one user at each provider organization must possess this role.**
EIM Reports *	• Users with this role may run and review reports. • *The role is appropriate for all staff members with access to invoice details (including the Personnel Summary Report).* • This role includes several reports: ✓ Activity PRC Detail Report by Service Category ✓ Activity PRC Detail Report by Service Code ✓ Activity PRC Detail Report by Claim ✓ Claim Summary Report by PRC ✓ PRC Payment Status Report ✓ Activity PRC Detail Report by Sub-Activity ✓ Ready Pay Reconciliation Report
Note: "*" indicates that at least one person in your organization must hold this role.	

EIM - Cost Reimbursement (CR) Roles	
Invoice Authorizer *	• This role allows a user to indicate final provider sign off on an invoice (payment voucher) prior to agency submission. • *Only users with signatory authority on the contract should be assigned this role.* • *This role should be given to a supervising fiscal executive (e.g. CFO, Fiscal Director, etc.).* • **At least one user at each provider organization must possess this role.**
Invoice Manager *	• This role allows users to create, edit and delete invoices (provided the status of the invoice permits these actions). Users with this role may release invoices to his/her provider Invoice Authorizer for approval. Additionally, they may create the Personnel Summary Report. • **At least one user at each provider organization must possess this role.**
Invoice Reviewer	• The role allows view-only access to cost reimbursement invoices, including Personnel Summary Report details. • It is typically given to executive leadership or managers who do not work directly with billing processes but need access to financial information. • *This role should be assigned to users who do not need to manage or authorize invoices.*
Cost Reimbursement SDR Manager	• This role allows users to manage, edit, copy and record a cost reimbursement service delivery report (SDR) and apply a service delivery pattern. • Users also have the ability to create and edit SDR Notes. • *Persons who hold this role must also be assigned either the Invoice Manager or Invoice Reviewer role.*
Cost Reimbursement SDR Reviewer	• This role allows view-only access to cost reimbursement contracts requiring service delivery reports (SDRs). • The role also allows SDR Notes to be viewed. • *Persons who hold this role must also be assigned either the Invoice Manager or Invoice Reviewer role.*

Invoice Assessment Manager	• This role allows users to update, complete, review, and edit invoice assessments. Invoice assessments are structured, online questionnaires that let providers respond to program-specific inquiries related to contract requirements and service deliverables. • *Known as "Service Delivery Reports" prior to EIM/ESM, invoice assessments are applicable only to select DPH and DMH contracts.* • *Persons who hold this role must also be assigned either the Invoice Manager or Invoice Reviewer role.*
Invoice Assessment Reviewer	• This role allows users to examine invoice assessments. Invoice assessments are structured, online questionnaires that let providers respond to program-specific inquiries related to contract requirements and service deliverables. • Known as *"Service Delivery Reports" prior to EIM/ESM, invoice assessments are applicable only to select DPH and DMH contracts.* • *Persons who hold this role must also be assigned either the Invoice Manager or Invoice Reviewer role.*
Ready Pay Invoice Reviewer	• This role grants view-only access to Ready Pay cost reimbursement invoices. • It is typically given to executive leadership or managers who do not work directly with billing processes but need access to financial information. • *It should be assigned to users who do not need to manage or authorize invoices.* • *The role is applicable only to select DMH, MRC and DMR providers.*
Cost Reimbursement Reports	• Users with this role are able to run and review reports. • *The role is appropriate for all staff members with access to cost reimbursement contracts and invoice details (including the Personnel Summary Report)*. • Several reports are included with this role: ✓ Commodity Based Payment Request Report ✓ Cost Reimbursement Budget Report ✓ Cost Reimbursement Expenditure Analysis Report ✓ Vendor Worksheet for Program (Activity) Budget Amendment Report ✓ Activity PRC Detail Report by Sub-Activity ✓ Cost Reimbursement Invoice Report ✓ Personnel Summary Report ✓ Cost Reimbursement SDR Report
Note: "*" indicates that at least one person in your organization must hold this role.	

EIM - Unit Rate (UR) Roles	
SDR Authorizer *	• This role authorizes Service Delivery Reports (SDRs), thus submitting them for agency review. It is the final level of provider SDR approval. • *This role should be given to a supervising fiscal executive (e.g. CFO, Fiscal Director, etc.).* • *Additionally, the SDR Authorizer role should always be given to staff employed at a central provider location.* • **At least one user at each provider organization must possess this role.**
SDR Location Manager *	• This role creates SDRs, enters time/attendance data, and applies service delivery patterns. • This role restricts access to editing header-level SDR fields (such as 'SDR Offset Amount') • *Thus, the role should be given to staff persons who need to complete the SDR and record time/attendance data (e.g. Case Worker, Site Billing Staff, etc.).* • *The SDR Location Manager role should be given to staff employed at service sites (to facilitate decentralized SDR completion).* • **At least one user at each provider organization must possess this role (or the SDR Manager role).**
SDR Manager *	• This role creates SDRs, enters time/attendance data, and applies service delivery patterns. • This role allows access to editing header-level SDR fields (such as 'SDR Offset Amount') • *Thus, the role should be given to staff persons who need to complete the SDR and record time/attendance data (e.g. Central Billing Staff, etc.).* • *The SDR Manager role should be given to staff employed at a central location (to facilitate centralized SDR completion).* • **At least one user at each provider organization must possess this role (or the SDR Location Manager role).**

SDR Release *	• This role releases the SDR to the SDR Authorizer for final provider approval. SDR release is done after time and attendance data entry at all locations is complete. • *Thus, the role should be given to staff persons who are responsible for the first level of SDR approval prior to submitting the SDR to the agency.* • *The SDR Release role should always be given to staff employed at a central provider location.* • **At least one user at each provider organization must possess this role.**
SDR Reviewer	• This role reviews the SDR and time/attendance data. It does not have the ability to change data on the SDR or change the status of the SDR. • *The role should be given to staff persons who have a need to view the SDR but not to modify any of the data it contains.*
Unit Rate Reports	• Users with this role are able to run and review reports. • Several reports are related to Unit Rate Contracts: ✓ Commodity Based Payment Request Report ✓ Payment Status Detail Report by Bed Days ✓ Payment Status Detail Report by Service Code ✓ Remittance Report by Bed Day ✓ Remittance Report by Service Code
SDR Reports	• Users with this role are able to run and review the SDR Report.
Accommodation Rate Invoice Authorizer	• This role authorizes accommodation rate invoices, thus submitting them for agency review. The role is the final level of provider invoice approval. • *It should be given to a supervising fiscal executive (e.g. CFO, Fiscal Director, etc.).*
Accommodation Rate Invoice Manager	• This role creates accommodation rate invoices. • *Thus, the role should be given to staff persons who need to complete accommodation rate invoices and enter invoice data (e.g. Billing Staff, etc.).*
Accommodation Rate Invoice Reviewer	• This role reviews the accommodation rate invoice. It does not have the ability to change data on the invoice or change the status of the invoice. • *This role should be given to staff members who have a need to view the invoice but not to modify any of the data it contains.*

Claim Authorizer (Select DPH programs only)	• This role may authorize batch claims (final approval before submission to a state agency for payment). • *This role should be given to a supervising fiscal executive (e.g. CFO, Fiscal Director, etc.).* • *Only users with signatory authority on the contract should be assigned this role.*
Claim Manager Inst (Select DPH programs only)	• This role has the ability to create and edit institutional (inpatient/residential) claims for submission to a state agency for payment. • The role can also release (first level of approval), correct and void a claim. • It also reviews explanation of benefits and authorization responses.
Claim Manager Prof (Select DPH programs only)	• This role has the ability to create and edit professional claims (outpatient/ambulatory) for submission to a state agency for payment. • The role can also release, correct and void a claim. • It also reviews explanation of benefits and authorization responses.
Claim Reviewer (Select DPH programs only)	• This role reviews claims (both professional and institutional) and explanation of benefits.
EIM WHN Reports	• Users with this role are able to run and review the Women's Health Network report called Fund Allocations by Service and Age Category (Fund Allocation Report)
Note: "*" indicates that at least one person in your organization must hold this role.	

ESM Roles	
Program Reviewer *	• Users with this review-only role may access client information, enrollments, credentials, consents, service plans, cases, invoices and final diagnoses. • *This role is applicable only to ESM users associated with the Department of Public Health.*
Intake Manager with Add	• This role manages client information, referrals, and enrollments. • It allows users to add clients, determine eligibility, create eligibility waiver requests and enroll clients in a particular program.
Intake Manager No Add	• This role manages client information, referrals, and enrollments. • The role does not allow a user to add clients; it is used for clients that have been created through Common Intake. • It allows users to determine eligibility, create eligibility waiver requests and enroll clients in a particular program.
Medical Record Manager Inst	• This role manages institutional (inpatient/residential) service records, service plans, notes and tasks, and final diagnosis results.
Medical Record Manager Prof	• This role manages professional (outpatient/ambulatory) service records, service plans, notes and tasks, and final diagnosis results.
Consent Manager	• This role has the ability to create informed electronic consents for the release of individual client information. These consents allow providers to transfer/share client demographic and/or service information between sites or programs. • This role may also review client information and service plans.
Enrollment Assessment Manager	• This role has the ability to create, update and review enrollment assessment data.
Enrollment Assessment Reviewer	• This role has read-only access to completed enrollment assessment data.
Disenrollment Assessment Manager	• This role has the ability to create, update and review disenrollment assessment data.
Disenrollment Assessment Reviewer	• This role has read-only access to completed disenrollment assessment data.
Service Assessment Manager	• This role has the ability to create and edit service plans, diagnosis assessment and screening assessment data.

Service Assessment Reviewer	• This role has read-only access to completed service plan, diagnosis assessment and screening assessment data.
Encounter Status Report (SBHC only)	• Provides the ability to print a copy of the unique daily encounters per site for each month of the selected year.
Aggregate Enrollment Status (SBHC only)	• Provides the ability to print a copy of the new unique client enrollments per site per month for the selected year.
Aggregate Service Report (SBHC only)	• Provides the ability to print a listing of the top 50 services delivered at a given site in a given period.
Aggregate Diagnosis Report (SBHC only)	• Provides the ability to print a listing of the top 50 diagnoses made at given site in a given period.
Diagnosis Report (SBHC only)	• Provides the ability to print a copy of the enrolled individuals associated with a selected diagnosis.
ESM Reports	• Users with this role are able to run and review reports. • Runs reports related to ESM include the ✓ Client Enrollment Status Report ✓ Client Extract Report ✓ Client with Abnormal Results Report ✓ Services Not Associated with a Claim or Have an Error Report ✓ Client with Incomplete Data Report
ESM WHN Reports	• Users with this role are able to run and review reports. • Reports related to Women's Health Network client data entered in ESM include the ✓ Client History – Heart Disease and Stroke Prevention Program ✓ Client History – Breast and Cervical Cancer Early Detection Program
Note: "*" indicates that at least one person in your organization must hold this role.	